# COUNTY OF LOS ANGELES
# DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

JOHN NAIMO
AUDITOR-CONTROLLER


June 3, 2015

TO: Supervisor Michael D. Antonovich, Mayor
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe

FROM: John Naimo
Auditor-Controller

SUBJECT: **ANNUAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY RULE PROGRAM REPORT FOR 2014**

This memo provides an annual update on the County's Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Program for the year ended December 31, 2014. The Office of the Chief HIPAA Privacy Officer (CHPO) and associated responsibilities reside with the Auditor-Controller (A-C). This report includes ongoing implementation efforts, modifications and new privacy-related regulations that impact the County's HIPAA Program, responsibilities imposed on covered departments by those changes, annual breach reports provided to the U.S. Department of Health and Human Services (HHS), and a list of recent audits completed by the CHPO.

## Background

The HIPAA Privacy Rule[1] provides important federal protections to protect the privacy of protected health information (PHI) and gives individuals rights with respect to that information. Covered entities and business associates may not use or disclose PHI, except as allowed by the Privacy Rule or with written authorization of the subject individual. The HIPAA Breach Notification Rule[2] requires HIPAA covered entities to

[1] 45 CFR Part 160 and Subparts A and E of Part 164
[2] 45 CFR Part 160 and Subparts A and D of Part 164

notify affected individuals, HHS, and in some cases, the media of the discovery of a breach of unsecured PHI.[3] This area of the CHPO's responsibilities is discussed below.

The CHPO faces challenges implementing ongoing changes to HIPAA and its related regulations. Additionally, programmatic and regulatory mandates require the CHPO to conduct ongoing reviews, respond to reported breaches and complaints, ensure departments are compliant with the Privacy Rule, and monitor workforce training. The departments, divisions, and commissions that are part of the County's health care component and must comply with HIPAA are:

- A-C's divisions and personnel who perform business associate functions
- Chief Executive Office
- Chief Information Office (CIO)
- County Counsel
- Executive Office of the Board, Children's Special Investigation Unit
- Executive Office of the Board, HIV Commission
- Department of Health Services (DHS)
- Department of Human Resources' (DHR) Employee Flexible Spending Accounts within the Employee Benefits Division
- Internal Services Department's (ISD) divisions and personnel who perform business associate functions
- Department of Mental Health (DMH)
- Probation Department – Electronic Medical Record System
- Department of Public Health (DPH)
- Treasurer and Tax Collector's divisions and personnel who perform business associate functions

**Ongoing Implementation of the Omnibus Rule**

On January 17, 2013, the Office for Civil Rights (OCR) of HHS issued the Omnibus Final Rule (Rule) implementing changes in regulations under HIPAA pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The changes were extensive and significantly strengthen privacy protections for patient health information while enhancing HHS' ability to enforce such protections. The Rule was effective on March 26, 2013, with a compliance date for most provisions of September 23, 2013.

While covered departments implemented and incorporated the changes into their Privacy Rule programs by HHS' deadline, we continue to work with them to ensure ongoing compliance with the regulations. Challenges for departments include information sharing and ensuring that internal and external contracts and agreements

[3] Unsecured PHI is any PHI that is not rendered or determined to unusable, unreadable, or indecipherable to an authorized individuals through the use of a technology or methodology.

include adequate safeguards related to ongoing compliance with the regulations. OCR recently developed model information-sharing agreements to promote health information exchanges, and began information-sharing with the State Attorney General on enforcement investigations concerning criminal violations of the HIPAA Privacy Rule. As discussed below, it appears that such violations are increasing. The CHPO works closely with the County Counsel to assist covered departments with Privacy Rule implementation and compliance challenges.

**Omnibus Rule Implementation of Business Associate Functions and Agreements**

When the HIPAA regulations were originally enacted, only covered entities were required to adhere to the law. That left many entities with access to PHI, such as billing agencies, information technology companies, and labs outside the scope and jurisdiction of HIPAA. Although covered entities were required to enter into agreements with these business associates to whom they provided medical information, HHS did not have jurisdiction to enforce or penalize business associates for non-compliance with HIPAA regulations. To address that enforcement gap, HIPAA was amended so that business associates (including County departments performing business associate functions) are now directly liable for HIPAA requirements related to safeguarding PHI and breach notification.

The HITECH Act also expanded the definition of business associate to include downstream subcontractors of business associates, and imposed direct liability on business associates and downstream vendors for violations of certain provisions, with maximum civil fines of up to $1.5 million per year. The CHPO worked with covered departments to ensure that business associate agreements were amended to include the updated language. In addition, ISD's master agreement now includes the revised HIPAA language.

**Omnibus Rule Breach Notification Requirements**

The Rule mandates that breaches of unsecured PHI be reported to HHS on an annual basis and to impacted individuals within 60 days of the discovery of a breach. If a breach of unsecured PHI impacts 500 or more individuals, covered entities must provide notice to both HHS and the impacted individuals without delay, but within 60 days of its discovery. Annual reports are due to HHS by March 1st for those breaches that impacted fewer than 500 individuals and occurred in the previous calendar year. For the 2014 calendar year, the County reported a total of 28 breaches to HHS, two of which were by business associates of the County. In comparison, a total of 11 breaches were reported to HHS and impacted individuals for 2013. The increase is primarily due to the changes in the regulations and reporting requirements that expanded the definition of a reportable breach.

## HIPAA Training Program

According to the regulations, the County must train workforce members on the HIPAA and HITECH Act and related policies and procedures to the extent necessary and appropriate for employees to carry out their functions without violating the regulations. The heath care component departments, with the exception of DHS, utilize the County's Learning Management System (LMS) to train their workforce members. DHS provides training through vendors, direct classroom instruction, and self-study guides. Approximately 35,000 County workforce members receive some form of HIPAA training each year, which includes updates and changes to the Privacy Rule regulations and relevant departmental policies.

At this time, the LMS-HIPAA training program does not include State or other privacy laws that may also apply to departments, specifically DHS. Thus, each department must develop training material that informs their employees about these additional privacy laws applicable to their operations. The CHPO provides assistance, guidance, and approves the departments' HIPAA training programs to the extent they include HIPAA Privacy Rule content. County Counsel is also part of the review and approval process, as well as the CIO if the content pertains to the Security Rule.

## HIPAA/HITECH Act Privacy and Security Committee

The CHPO and the County's Chief Information Security Officer jointly established a HIPAA/HITECH Act Privacy and Security Committee (Committee) consisting of representatives from each of the health care component departments. County Counsel is also an active participant on the Committee, and provides updates on legal requirements impacting the Privacy Rule program and covered departments. The Committee meets monthly to discuss changes in regulations, implementation and standard requirements, updates to privacy and security policies and procedures, enforcement, and proposed/upcoming laws and policies that may impact the covered departments' HIPAA programs.

## HIPAA Privacy Rule Audits Conducted in 2014

A key responsibility of the CHPO is to conduct audits and reviews to ensure that covered entities are complying with the Privacy Rule. For calendar year 2014, the audits/reviews took place for the following programs:

- DMH: Rio Hondo Mental Health Center
- DMH: Roybal Mental Health Center
- DPH: Nurse Family Partnership Program
- DPH: Torrance Public Health Center
- DHS: Harbor-UCLA Medical Center

The CHPO also conducts unannounced site visits to ensure that County clinics and hospitals are posting their notices of privacy practices according to HIPAA standards, and meeting other observable privacy program requirements. For the 2014 calendar year, the CHPO visited 11 facilities, of which four were found to have minor compliance issues. If there is a finding that a facility or program is not in compliance with the regulations or standards, the CHPO coordinates with the department's designated privacy and/or compliance officers in the development of a corrective action plan. Follow-up activity takes place until all issues are adequately resolved.

**HIPAA Privacy Complaints and Investigations**

HIPAA requires covered entities to establish a process for individuals to complain if they believe their privacy rights have been violated. Further, there must be a process to document complaints, allegations, breaches, and queries by anyone including constituents, patients, agencies, workforce members, and OCR. Complaints are received by the CHPO through the HIPAA Hotline (213) 974-2164, a dedicated HIPAA e-mail address (hipaa@auditor.lacounty.gov), in-person, and by mail. Covered departments also maintain a log of complaints that are reported to the CHPO, should the incident be determined to be reportable to the HHS.

For calendar year 2014, the CHPO's office logged 72 complaints, representing a 31% increase from 2013, when 55 complaints were received. Complaints and issues were resolved, and reported accordingly or pending action from another agency, such as HHS. The most common complaints against the County involved allegations of wrongful disclosure of PHI and County employees accessing medical records without a business need. The most common incidents that were reported by departments to the CHPO involved the loss/theft of computer devices, or loss of paper files that contained PHI.

**Enforcement and Penalties for Non-compliance**

HHS enforces HIPAA and the HITECH Act and may issue fines and penalties with civil fines of up to $1.5 million per incident. HHS considers a number of factors in deciding whether to issue fines and penalties for a breach, including the adequacy of the covered entity's compliance infrastructure. To date, despite a number of reportable breaches, no penalties have been issued by HHS against the County for non-compliance.

**Emerging Trends**

As mentioned in earlier reports to your Board, the scope and responsibilities of the CHPO were significantly impacted with the passage of the HITECH Act in 2009, which established the Breach Notification Rule. When a large privacy breach is suspected, the CHPO, staff, and departmental staff must respond immediately to comply with the regulations and mitigate any harm to individuals and the County. When criminal activity

is suspected, law enforcement agencies become a significant component of the mitigation effort. The County's largest breaches have been due to criminal activity, which the CHPO works closely with the A-C's Office of County Investigations' (OCI) investigators and other law enforcement agencies.

In recent years, we have observed within the County an increase in criminal activity involving patient PHI. For the calendar year 2014 the CHPO logged 11 incidents related to criminal activity, representing a 175% increase from 2013, when four incidents were received. To ensure that the A-C is prepared to respond to such incidents, the CHPO resides organizationally within OCI. This ensures that appropriate resources and trained staff are available to investigate breaches of PHI that involve various forms of fraud. The CHPO and OCI coordinate the County's response to any theft of our clients' PHI, and we work with law enforcement agencies in their investigations, as well as County Counsel. This immediate and in-depth response to breaches involving a criminal component has had a notable impact on our changing roles to meet the demands of an investigation while maintaining compliance with HIPAA, federal, State, and the breach notification regulations.

**Next Steps**

The CHPO and the Committee have drafted Board HIPAA policies to ensure that covered departments and staff are aware of and comply with the HIPAA requirements. The draft policies include the minimum requirements for employee HIPAA training, safeguarding PHI, and discipline of workforce members who do not comply with the Privacy and Security Rules. While the covered departments have HIPAA policies that address these requirements, the purpose for developing the countywide policies is to establish a consistent standard throughout the covered entity. We anticipate clearing these policies with staff and submitting them to your Board by December 2015.

The CHPO plans to develop a tool for use in routine audits of business associates of covered departments, to evaluate their compliance with HIPAA requirements as part of the County's ongoing contract monitoring and fiscal reviews. Currently, the regulations do not require covered entities to monitor their business associates for compliance with HIPAA. However, if a covered entity observes a pattern of non-compliance with the regulations, such as not safeguarding PHI, then the covered entity has an obligation to request assurances that the business associate will comply with the regulations. This audit tool will be available to contract monitoring and audit staff to document any issues observed during audits of business associates.

**Summary and Conclusion**

The CHPO continues to advance awareness of health privacy matters through leadership of the Committee, ongoing training, audits, and by providing technical assistance and expertise to covered departments. The CHPO is responsive to

departments, individuals, workforce members, business associates, privacy and security taskforces, HHS, and your Board in resolving privacy complaints and concerns. The CHPO will continue to work with the covered departments to implement future changes to the regulations, and to identify and address compliance issues and public complaints.

Please call me if you have questions, or your staff may contact Linda McBride, CHPO, at (213) 974-2166.

JN:RGC:GZ:LTM

c: Sachi A. Hamai, Interim Chief Executive Officer
James McDonnell, Sheriff
Patrick Ogawa, Acting Executive Officer
Mark J. Saladino, County Counsel
Mitchell H. Katz, M.D., Director, Department of Health Services
Cynthia Harding, Interim Director, Department of Public Health
Marvin J. Southard, D.S.W., Director, Department of Mental Health
Jerry E. Powers, Chief Probation Officer
Lisa M. Garrett, Director of Personnel, Department of Human Resources
Richard Sanchez, Chief Information Officer
Dave Chittenden, Chief Deputy Director, Internal Services Department
Joseph Kelly, Treasurer and Tax Collector
Craig A. Vincent-Jones, Executive Director, Commission on HIV, Executive Office of the Board
Kimberly Wong, Lead Attorney, Children's Special Investigation Unit, Executive Office of the Board